Distribution of the zeros of certain self-reciprocal polynomials (Analytic Number Theory and Related Areas)

AUTHOR(S):

知念, 宏司

CITATION:

知念, 宏司. Distribution of the zeros of certain self-reciprocal polynomials (Analytic Number Theory and Related Areas). 数理解析研究所講究録 2009, 1665: 9-16

ISSUE DATE:

2009-10

URL:

http://hdl.handle.net/2433/141059

数理解析研究所講究録
第1665巻 2009年 9-16

Distribution of the zeros of certain self-reciprocal polynomials

近畿大学　理工学部　知念 宏司 (Koji Chinen)
Department of Mathematics, School of Science and Engineering, Kinki University.

概 要

実数係数の多項式 $f(T)=\sum_{i=0}^{n}a_iT^i$ が $a_i=a_{n-i}$ $(\forall i)$ を満たすとき, $f(T)$ を自己相反多項式 (self-reciprocal polynomial) という. 本稿では, 自己相反多項式がすべての根を単位円周上にもつための, 1つの十分条件を与える. 応用として, ある種の誤り訂正符号に関連する不変式の Riemann 予想にも触れる.

Summary

A real polynomial $f(T)=\sum_{i=0}^{n}a_iT^i$ is called self-reciprocal if $a_i=a_{n-i}$ $(\forall i)$ is satisfied. In this article, we give a certain sufficient condition for a self-reciprocal polynomial to have all the roots on the unit circle. As an application, we will mention the Riemann hypothesis for invariant polynomials related to certain error-correcting codes.

1 主結果

まず次の定義から出発する:

定 義 1.1 実数係数の多項式 $f(T)=\sum_{i=0}^{n}a_iT^i$ が任意の i $(0\leq i\leq n)$ に対して $a_i=a_{n-i}$ を満たすとき, $f(T)$ を自己相反多項式 (self-reciprocal polynomial) という.

つまり, 係数が「回文 (palindrome)」となっているものである. この性質は self-inversible と呼ばれることもある. また, 自己相反多項式 $f(T)$ に対し, 方程式 $f(T)=0$ は「相反方程式 (reciprocal equation)」と呼ばれる. 次が本稿の主結果である:

定 理 1.2 多項式 $f(T)=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m$ $(m>2k)$ が $a_0>a_1>\cdots>a_k>0$ を満たすなら, $f(T)$ の根はすべて単位円周上にある.

これは, 次の古典的結果の自己相反多項式への拡張とも言えるもので, 主張を見比べてみるとなかなかおもしろい:

定 理 1.3 (Eneström - 掛谷) 多項式 $f(T)=a_0+a_1T+\cdots+a_kT^k$ が $a_0>a_1>\cdots>a_k>0$ を満たすなら, $f(T)$ の根はすべて単位円周の外側 $(|T|>1)$ にある.

注 意. Eneström - 掛谷の定理は次の形で述べられることも多い: 「多項式 $f(T)=a_0+a_1T+\cdots+a_kT^k$ が $a_0\geq a_1\geq\cdots\geq a_k>0$ を満たすなら, $f(T)$ の根はすべて単位円の周または外側 ($|T|\geq 1$) にある」([2, p.12] など). つまり係数の間の不等式が等号つきかそうでないかが単位円周上の根の存在可能性に影響する. 定理 1.3 の形で述べている文献はむしろ少数派だが, 例えば Marden [17, p.151, Exercise 4], 楠 [14, p.14, 練習問題 5] にある. このうち [14] の証明は, 三角不等式の等号成立条件を詳しく見ることで得られる初等的証明である.

定理 1.2 は, ある種の zeta 関数の Riemann 予想を考察する過程で得られた. つまり, 種々の合同 zeta 型の zeta 関数は, その分子となる多項式 $P(T)$ に変数変換 $T\mapsto T/\sqrt{q}$ (q は関連する有限体の元の個数) を施すと関数等式の帰結として自己相反多項式が現れる. その場合, $P(T/\sqrt{q})$ (自己相反) のすべての根が単位円周上にあることと, もとの zeta 関数が Riemann 予想を満たすこととが同値となる. 筆者は最近, ある誤り訂正符号から得られる不変式の zeta 関数の系列に対し, 定理 1.2 を用いて Riemann 予想が成立することを示した. これについては第 3, 4 節で述べる. なお, 本稿の結果について, より詳しくは [7] を参照. また, 自己相反多項式の根の分布 (特に単位円周上) について論じた比較的新しい文献として, 例えば [8] などもある.

謝 辞. 主結果を導くにあたって, 村田玲音氏, 鈴木正俊氏との議論は大変有益であった. また研究集会当日, 若林功氏, 金子元氏は大変貴重なご意見を下さった. 心より感謝を申し上げたい.

2 定理 1.2 の証明

さて, 多項式

$$f(T)=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m\quad(m>2k)\quad(2.1)$$

が $a_0>a_1>\cdots>a_k>0$ を満たしているとしよう. $f(T)$ を 2 つの多項式

$$\begin{aligned}P(T)&:=a_0+a_1T+\cdots+a_kT^k,\\ Q(T)&:=a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m,\end{aligned}\qquad(2.2)$$

の和で $f(T)=P(T)+Q(T)$ と表す. このとき仮定 $a_0>a_1>\cdots>a_k>0$ から, 定理 1.3 により $P(T)$ は $|T|\leq 1$ に根を持たないことがわかる. この $P(T)$, $Q(T)$ に対して, 次が成り立つ:

定 理 2.1 単位円の内部 $|T|<1$ において $|P(T)|>|Q(T)|$.

これが言えれば, $|T|<1$ において $f(T)=P(T)+Q(T)\neq 0$ がわかる. 実際, もし $f(T)=0$ となるなら, $P(T)=-Q(T)$, したがって $|P(T)|=|Q(T)|$ ($\exists T$, $|T|<1$) となり, 定理 2.1 に矛盾する. ところで, $f(T)$ が自己相反という仮定から

$$T^m f\left(\frac{1}{T}\right)=f(T)$$

が成り立つ. この式は, 単位円の内部にある $f(T)$ の根と単位円の外部にある $f(T)$ の根が 1 対 1 に対応することを示しており (α が根ならば $1/\alpha$ も根), このことと $f(T) \neq 0$ ($|T| < 1$) を合わせると, $f(T)$ は単位円の内部にも外部にも根を持たないこと, つまりすべての根が単位円周上にあることがわかり, 定理 1.2 が示せることとなる.

定理 2.1 の証明

まず次を示そう:

補 題 2.2 式 (2.2) の $P(T)$, $Q(T)$ に対し, $|T| = 1$ 上で

$$|P(T)| = |Q(T)|.$$

証 明. $T = e^{i\theta}$ とおくと, $|P(e^{i\theta})| = |\sum_{j=0}^{k} a_j e^{ij\theta}| = |\sum_{j=0}^{k} a_j e^{-ij\theta}| = |\sum_{j=0}^{k} a_j e^{i(m-j)\theta}|$ $= |Q(e^{i\theta})|$. ∎

さらに次のよく知られた結果を準備する:

定 理 2.3 (最大値の原理) 関数 $g(T)$ は有界領域 $D \subset \mathbf{C}$ で正則かつ非定数, $\overline{D}$ (D の閉包) で連続とする. すると $|g(T)|$ はその最大値 M を $\overline{D} - D$ 上でとり, しかも D において

$$|g(T)| < M.$$

証 明. Ahlfors [1, p.134]. ∎

さて, 定理 2.3 を関数 $g(T) := Q(T)/P(T)$, 領域 $D := \{T \in \mathbf{C}\ ;\ |T| < 1\}$ に対して適用する. 明らかに $g(T)$ は有理型かつ非定数. しかも定理 1.3 より $g(T)$ は $\overline{D}$ 上で極を持たない. さらに補題 2.2 より, D の境界上で $|g(T)| = 1$. したがって定理 2.3 により D の内部で $|g(T)| < 1$ となることがわかり定理 2.1 が得られる.

注 意. (1) 定理 1.2 はいろいろな variation が可能である. 例えば仮定 $m > 2k$ はそれほど本質的でなく, $Q(T) = a_k T^l + a_{k-1} T^{l+1} + \cdots + a_0 T^{k+l}$ ($l \geq 0$) の形なら証明はそのまま当てはまる (鈴木正俊氏の指摘).

(2) 上の証明では $g(T)$ が単位円周上に極を持たないことを本質的に使っているが, 今の場合 $P(T)$ が単位円周上に零点を持てば, それは $Q(T)$ の零点でもあり (零点の位数も一致), $g(T)$ の単位円周上の特異点は除去可能となる. したがって §1 の注意で述べた, 弱い形の Eneström - 掛谷の定理で代用することも実は可能である (金子元氏の指摘).

(3) 上記 (1), (2) を考慮すると, 次の形まで一般化可能である: 「自己相反多項式 $f(T)$ が $f(T) = P(T) + T^k P(1/T)$ ($P(T)$ は実数係数多項式で $k \geq \deg P$) の形で表され, $P(T)$ が $|T| < 1$ に根を持たないとき, $f(T)$ のすべての根は単位円周上にある.」これはいろいろな場面に応用できるであろう.

3 符号の zeta 関数とその不変式への拡張

線型符号の zeta 関数は, 1999 年, Iwan Duursma によって定義された ([9]). C を有限体 $\mathbf{F}_q$ ($q=p^r$, p: 素数, $r\geq 1$) 上の $[n,k,d]$-線型符号とし (つまり C は ${\mathbf{F}_q}^n$ の k 次元部分ベクトル空間),

$$W_C(x,y)=x^n+\sum_{i=d}^{n}A_i x^{n-i}y^i \qquad (A_d\neq 0)$$

をその重み多項式とする (符号理論の (数学的) 一般論に関して, 標準的な教科書の 1 つは [18], また [15, pp. 471-496] は簡単な入門として手軽である). なお, この d は C の最小距離と呼ばれ, 符号の誤り訂正能力を決定づける (d が大きいほど訂正能力が高い).

定 義 3.1 C に対して, 次数 $n-d$ 以下のある多項式 $P(T)\in\mathbf{Q}[T]$ がただ 1 つ存在して,

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n=\cdots+\frac{W_C(x,y)-x^n}{q-1}T^{n-d}+\cdots$$

が成立する. $P(T)$ を C の **zeta 多項式**, $Z(T):=P(T)/\{(1-T)(1-qT)\}$ を C の **zeta 関数**と呼ぶ.

多項式 $P(T)$ の存在と一意性に関しては, Duursma の論文にはあまりわかりやすい形で書かれていないが, 初等的証明が筆者らの総合報告 [4, pp.92-93], [13, p.44], [5, pp.32-33] にある. また [7, Appendix A] も参照.

この定義にいう「符号の zeta 関数」に関して詳しいことは Duursma の論文 [10], [11] あるいは [4], [13] などをご参照いただきたいが, 彼の一連の結果のうち筆者にとって特に興味深いのは自己双対符号の zeta 多項式に対する関数等式

$$P(T)=P\Big(\frac{1}{qT}\Big)q^gT^{2g} \tag{3.1}$$

である ($g=n/2+1-d$). ここで, C が自己双対とは, ${\mathbf{F}_q}^n$ の通常の内積に関して, $C^\perp=C$ となる (直交補空間が自分自身と一致する) ことである. これは代数曲線の zeta 多項式 (いわゆる合同 zeta 関数の分子) がもつ関数等式と全く同じ形であり, したがって「符号の Riemann 予想」を次のように定式化できる:

定 義 3.2 C を自己双対符号, その zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 α に対して,

$$|\alpha|=\frac{1}{\sqrt{q}}$$

が成り立つとき, C は Riemann 予想を満たすという.

符号の Riemann 予想はすべての自己双対符号によって満たされるわけではなく, 実在の自己双対符号で Riemann 予想を満たすもの, 満たさないもの, 両方の実例が存在する. 符号が Riemann 予想を満たすための必要十分条件を求めることはまだ未解決であるが, Duursma は

問 題 3.3 「Extremal な自己双対符号は Riemann 予想を満たす」は正しいか.

という問題を提出している ([11]). ここで, $\mathbf{F}_q$ 上の同じ符号長の自己双対符号のうち, 最小距離が最大のものを extremal という ([18, p.139]). 最小距離が大きいほど訂正能力は高いわけだから, extremal という性質は応用上からもよい性質である. そして Duursma は, いわゆる Type IV 自己双対符号に関してはこれを肯定的に解決している ([12]). なお第 1 節で述べた通り, 関数等式 (3.1) の帰結として, zeta 多項式 $P(T)$ に変数変換 $T \mapsto T/\sqrt{q}$ をほどこした $P(T/\sqrt{q})$ は自己相反多項式となることがわかり, こうして zeta 多項式と自己相反多項式が関連づけられる. そして, Duursma による Type IV extremal 自己双対符号に対する Riemann 予想証明法は, 自己相反化した zeta 多項式 $P(T/\sqrt{q})$ をある種の変数変換で Gegenbauer 多項式 (別名 ultraspherical polynomials, 直交多項式系の一種) に関連づけ, その根の分布から $P(T/\sqrt{q})$ の単位円周上の根の分布を調べるという, まことに巧妙なものであった.

注 意. 最近では extremal code の定義はさらに限定されて, $\mathbf{F}_2$, $\mathbf{F}_3$ または $\mathbf{F}_4$ 上の自己双対符号で, Mallows-Sloane 限界式 ([12, §1.1]) を等号で満たすもの, とすることが多い.

さて, 定義 3.1 を見てみると, $P(T)$ の存在と一意性の証明においては, $W_C(x,y)$ が実在する符号の重み多項式であることよりも, それが x, y **の斉次** n **次式であることがより本質的**であることがわかる. この事実はすでに MDS 符号 (最大距離分離符号) の zeta 関数の考察において Duursma 自身によっても暗に用いられているが, 筆者はより積極的にこの点に注目し, 必ずしも符号と関連をもたない複素数係数の斉次多項式

$$W(x,y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \quad (A_d \neq 0) \tag{3.2}$$

に対してその zeta 多項式 $P(T)$ を, 全く同様に定義できることを指摘した ([5, p.40]. また [7, Appendix A] も参照).

さらに, $P(T)$ の関数等式はどこから来るかというと, $W(x,y)$ が

$$\sigma_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \tag{3.3}$$

で不変であるという事実の帰結である. ここで, 1 次変換 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の多項式 $f(x,y)$ への作用は $f^\sigma(x,y) = f(ax+by, cx+dy)$ とする. 実在する符号の場合, C が $\mathbf{F}_q$ 上の自己双対符号ならばその重み多項式は $W_C{}^{\sigma_q}(x,y) = W_C(x,y)$ を満たすことが知られている.

ところで, σ_q で不変な $W(x,y)$ 全体 (不変式環) の構造は知られていて,

$$\mathbf{C}[x,y]^{\langle \sigma_q \rangle} := \{W(x,y) \in \mathbf{C}[x,y] \ ; \ W(x,y)^{\sigma_q} = W(x,y)\} = \mathbf{C}[x + (\sqrt{q}-1)y, y(x-y)]$$

である (MacWilliams-Sloane [16, p.605, Theorem 5]). そこで, $P(T)$ が関数等式 (3.1) を満たすような $W(x,y)$ を考えるには, $\mathbf{C}[x,y]^{\langle \sigma_q \rangle}$ の元を考えればよい. こうして「不変式の Riemann 予想」を考えることができる:

定 義 3.4 $W(x,y) \in \mathbf{C}[x,y]^{\langle \sigma_q \rangle}$ は (3.2) の形の斉次多項式とし, $W(x,y)$ の zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, $W(x,y)$ は Riemann 予想を満たすという.

注 意. (1) $W(x,y)$ が σ_q 不変でなくても (したがって対応する $P(T)$ は関数等式を満たさない) Riemann 予想を満たす, という例もあるにはある. $\mathbf{F}_2$ 上の [7,4,3] Hamming 符号の重み多項式がその一例である.

(2) 少し違った形の関数等式 $P(T) = -P(\frac{1}{qT})q^gT^{2g}$ (マイナスがつく) を満たす不変式もあり (もちろん $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ とは別の不変式環の元), やはり Riemann 予想を満たすものの実例が見つかっている ([6]).

4 一般 Hamming 符号から得られる不変式とその Riemann 予想

不変式環 $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ において, 定義 3.4 の意味で Riemann 予想を満たすものをできるだけたくさん見つける, という問題を考える. 筆者は [7] において, 必ずしも自己双対ではない符号の重み多項式から不変式を作ることにより, そのような例を無限個構成した. 以下, 結果だけを述べる.

$\mathbf{F}_q$ 上の線型符号 C とその双対符号 $C^\perp$ は重み多項式に次の関係がある (MacWilliams の等式, [16, p.146, Theorem 13]):

$$W_C^{\sigma_q}(x,y) = q^{k-n/2}W_{C^\perp}(x,y) \quad \text{または} \quad W_{C^\perp}^{\sigma_q}(x,y) = q^{n/2-k}W_C(x,y)$$

そこで

$$\tilde{W}_C(x,y) := \frac{1}{1+q^{k-n/2}}\{W_C(x,y) + q^{k-n/2}W_{C^\perp}(x,y)\} \tag{4.1}$$

とすれば $W_C(x,y)$ と $W_{C^\perp}(x,y)$ が「互いに移りあう」ことにより, $\tilde{W}_C(x,y)$ は σ_q 不変, つまり $\tilde{W}_C(x,y) \in \mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ となり, しかも (3.2) の形となる. こうして任意の線型符号 C から不変式を作ることができる.

そこで符号 C として, 一般 Hamming 符号をとる. これは $r \geq 2$ と任意の $\mathbf{F}_q$ に対して定義される符号で, パラメータ $[(q^r-1)/(q-1) = n, n-r, 3]$ をもつ (r と q とで決まる. 詳しくは Brouwer [3, p.316]). 重み多項式 $W_C(x,y)$ はかなり複雑だが, 双対符号 $C^\perp$ の重み多項式は

$$W_{C^\perp}(x,y) = x^n + (q-1)nx^{\frac{n-1}{q}}y^{\frac{(q-1)n+1}{q}}$$

と, 比較的簡単な形をしている. これがわかれば以後の計算には十分である.

この C に対して上の方法で不変式 $\tilde{W}_C(x,y)$ を作ると, $r \geq 2$ のとき, $\tilde{W}_C(x,y)$ の zeta 多項式 $\tilde{P}_{r,q}(T) := \tilde{P}_C(T)$ は

$$\tilde{P}_{r,q}(T) = \frac{N_{r,q}}{1+q^{r-n/2}}(F_1(T) - qF_2(T)),$$

ただし, $N_{r,q} = n/\binom{n}{q^{r-1}}$ で,

$$F_1(T) = \sum_{i=0}^{n-d-1} \binom{n-i-2}{d-1} q^{i+2-n/2} T^i + \sum_{i=d-3}^{n-4} \binom{i+2}{d-1} T^i,$$
$$F_2(T) = \sum_{i=0}^{n-d-2} \binom{n-i-3}{d-1} q^{i+2-n/2} T^i + \sum_{i=d-2}^{n-4} \binom{i+1}{d-1} T^i$$

と計算される ([7, Theorem 4.5]). これを $T \mapsto T/\sqrt{q}$ で正規化した $\tilde{P}_{r,q}(T/\sqrt{q})$ は自己相反である. 実は $r \geq 3$, $q \geq 4$ のときには $\tilde{P}_{r,q}(T/\sqrt{q})$ の係数は定理 1.2 の仮定を満たすこと, したがってすべての根が単位円周上にあることが証明でき, その結果, 次が示せる:

定 理 4.1 $r \geq 3$ かつ $q \geq 4$ のとき, 一般 Hamming 符号 C から (4.1) によって得られる不変式は定義 3.4 の意味で Riemann 予想を満たす.

注 意. (1) $r = 2$ の場合, 一般 Hamming 符号は MDS 符号と呼ばれるものになり, 全く違う方法でその不変式の Riemann 予想が証明できる ([7, §3]). したがって, $r = 3$, $q = 2, 3$ の場合が証明されずに残っているが, 数値実験によると, その場合も不変式の Riemann 予想は成立するように見える.

(2) [7] では, C が MDS 符号のとき, そして Golay 符号 (自己双対でないもの, 2 つある) のときにも, 上の方法で作った不変式が Riemann 予想を満たすことを示した ([7, §3, §7]). ところで, ある種の MDS 符号, 一般 Hamming 符号, Golay 符号は「完全符号」(Pless [18, p.21]) という効率的な一群の符号を形成し, 応用上も重要なものである. 実在の符号 C から (4.1) によって得られる不変式, およびその Riemann 予想が応用上意味を持つのかどうか, まだわからない. しかし完全符号から得られる不変式がそろって Riemann 予想を満たす (一部は予想だが), という現象にはちょっと興味を惹かれる. さらに完全符号以外の MDS 符号も存在するときには非常によい符号となる. 定義 3.4 の Riemann 予想が符号の何らかのよい性質を反映している可能性もなくはない気がする.

Submitted on , 2008.

参考文献

[1] Ahlfors, L. V. : Complex Analysis, third ed., McGraw-Hill, NewYork, 1979.

[2] Borwein, P. and Erdélyi, T. : Polynomials and Polynomial Inequalities, GTM 161, Springer, 1995.

[3] Brouwer, A. E. : Bounds on the size of linear codes, in V. S. Pless, W. C. Huffman (eds.), Handbook of Coding Theory, I, II, Elsevier Science B. V., Amsterdam, 1998, 295-461.

[4] 知念 宏司, 平松 豊一 : 線形符号のゼータ関数とリーマン予想の類似 (Iwan Duursma の仕事の紹介), 符号と暗号の代数的数理, 京都大学数理解析研究所講究録 1361 (2004), 91-101.

[5] 知念 宏司 : 線型符号のゼータ関数とそのリーマン予想 (Iwan Duursma の仕事の紹介, 及び 1 つの拡張), 仙台数論及び組合せ論小研究集会 2004 報告集 (2005), 31-44.

[6] Chinen, K : Zeta functions for formal weight enumerators and the extremal property, Proc. Japan Acad. **81** Ser. A. (2005), 168-173.

[7] _____ : An abundance of invariant polynomials satisfying the Riemann hypothesis, to appear in Discrete Math.

[8] DiPippo, S. A. and Howe, E. W. : Real polynomials with all roots on the unit circle and abelian varieties over finite fields, J. Number Theory **73** (1998), 426-450, corrigendum, ibid. **83** (2000), 182.

[9] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[10] _____ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[11] _____ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[12] _____ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[13] 平松 豊一, 知念 宏司 : 線形符号のゼータ関数とそのリーマン予想, 特集「符号化理論の新時代」, 数理科学 **497** (2004), 42 - 47.

[14] 楠 幸男: 解析函数論, 廣川書店, 1962 年.

[15] Lidl, R. and Niederreiter, H. : Finite Fields, Encyclopedia of Mathematics and its Applications vol. 20, Addison-Wesley, 1983.

[16] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[17] Marden, M. : The Geometry of the Zeros of a Polynomial in a Complex Variable, Math. Surveys 3, Amer. Math. Soc., 1949.

[18] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).